

FIG. 1

```
graph TD; 100[Receiving a user id, which uniquely identifies an account at a server] --> 110[Generating a random number Nr]; 110 --> 120[Calculating the designated password Pd according to the password transform algorithm]; 120 --> 130[Computing a hash value of the user id, the common password, and the server name]; 130 --> 140[Using the hash value to form a symmetric key Kr]; 140 --> 150[Encrypting the random number Nr with the symmetric key Kr, by using some symmetric encryption algorithm]; 150 --> 160[Submitting the user id, the designated password Pd, and the encrypted random number Kr(Nr) to the server via a secure connection,]; 160 --> 170[Hashing the designated password Pd and saving the user ID, hash value of the designated password Hash(Pd), and the encrypted random number Kr(Nr) into a password file];
```

Receiving a user id, which uniquely identifies an account at a server 100

Generating a random number Nr 110

Calculating the designated password Pd according to the password transform algorithm 120

Computing a hash value of the user id, the common password, and the server name 130

Using the hash value to form a symmetric key Kr 140

Encrypting the random number Nr with the symmetric key Kr, by using some symmetric encryption algorithm 150

Submitting the user id, the designated password Pd, and the encrypted random number Kr(Nr) to the server via a secure connection, 160

Hashing the designated password Pd and saving the user ID, hash value of the designated password Hash(Pd), and the encrypted random number Kr(Nr) into a password file 170

FIG. 2

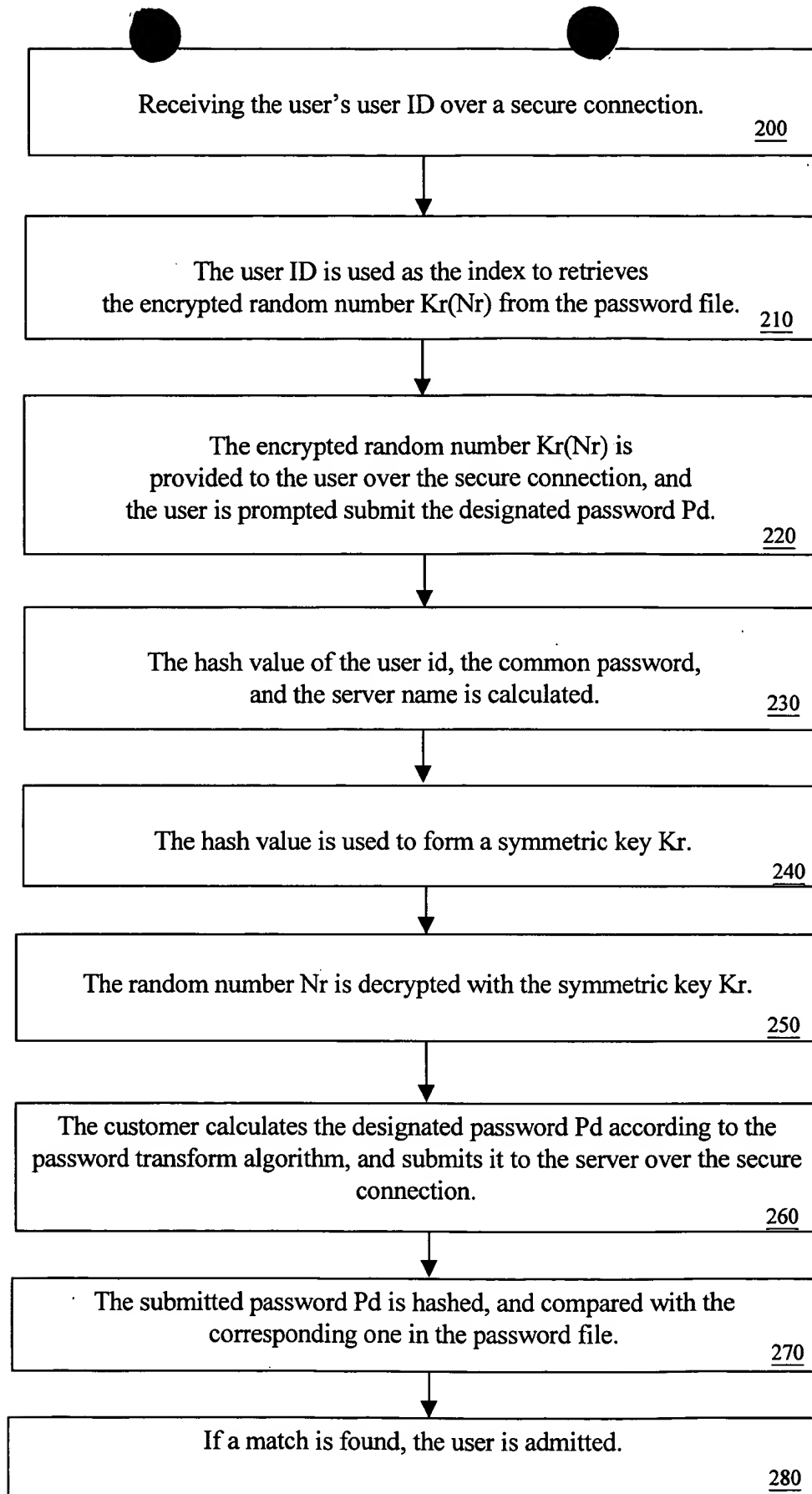


FIG. 3

```
graph TD; 300[Generating a new random number N'r] --> 310[Calculating the new designated password P'd in terms of the user id, the common password, the server name, and the new random number N'r]; 310 --> 320[Encrypting the new random number N'r by using the same symmetric key Kr]; 320 --> 330[Submitting the new designated password P'd and the encrypted new random number Kr(N'r), along with the old designated password Pd to the server over the secure connection]; 330 --> 340[Validating the submitted password Pd and updating the password file by replacing the hash value of the old designated password Hash(Pd) and the encrypted version of the old random number Kr(Nr) with the correspondingly new ones];
```

Generating a new random number $N'r$ 300

↓

Calculating the new designated password $P'd$ in terms of the user id, the common password, the server name, and the new random number $N'r$ 310

↓

Encrypting the new random number $N'r$ by using the same symmetric key Kr 320

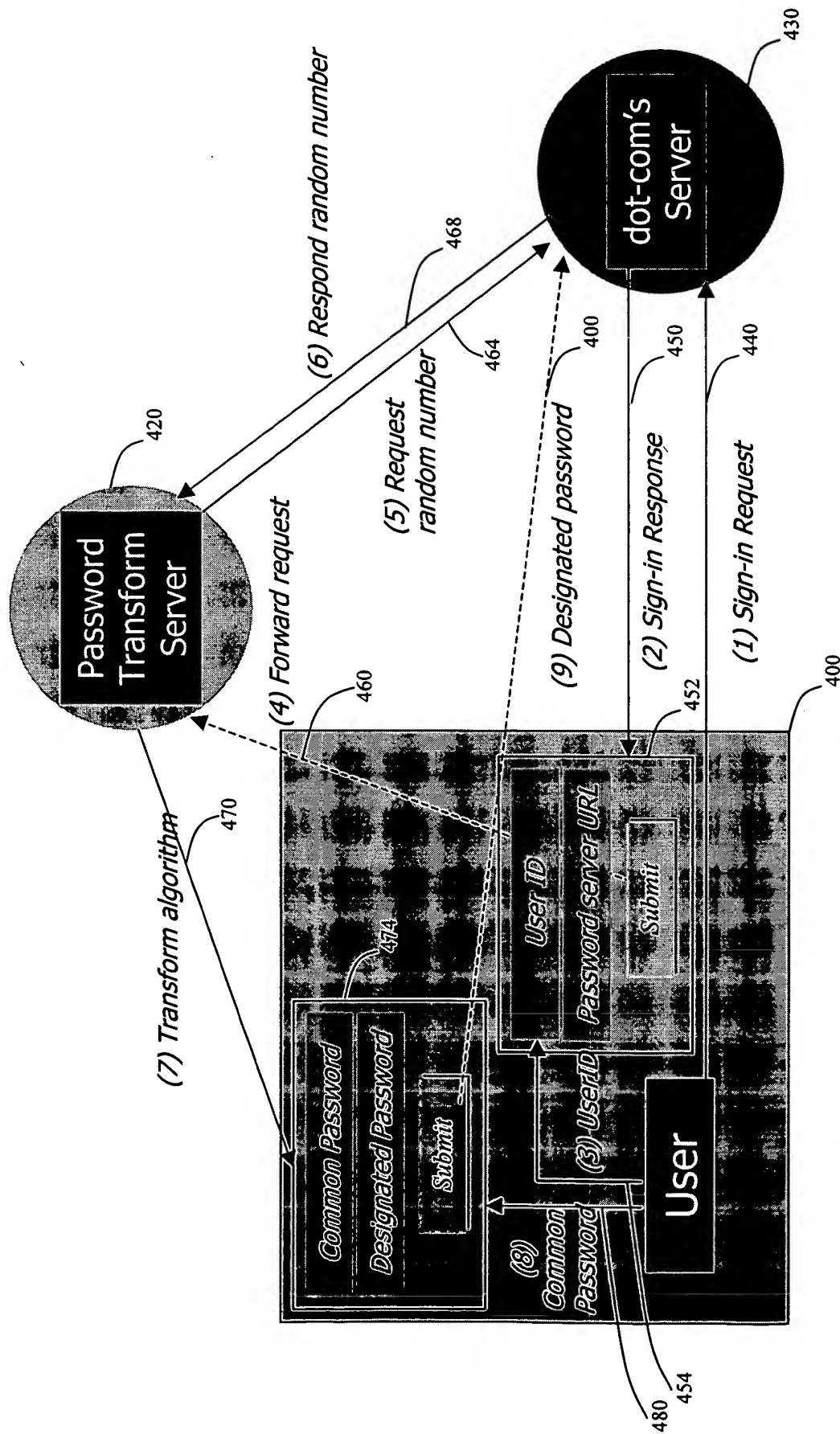
↓

Submitting the new designated password $P'd$ and the encrypted new random number $Kr(N'r)$, along with the old designated password Pd to the server over the secure connection 330

↓

Validating the submitted password Pd and updating the password file by replacing the hash value of the old designated password $Hash(Pd)$ and the encrypted version of the old random number $Kr(Nr)$ with the correspondingly new ones 340

FIG. 4



Best Available Copy

FIG. 5

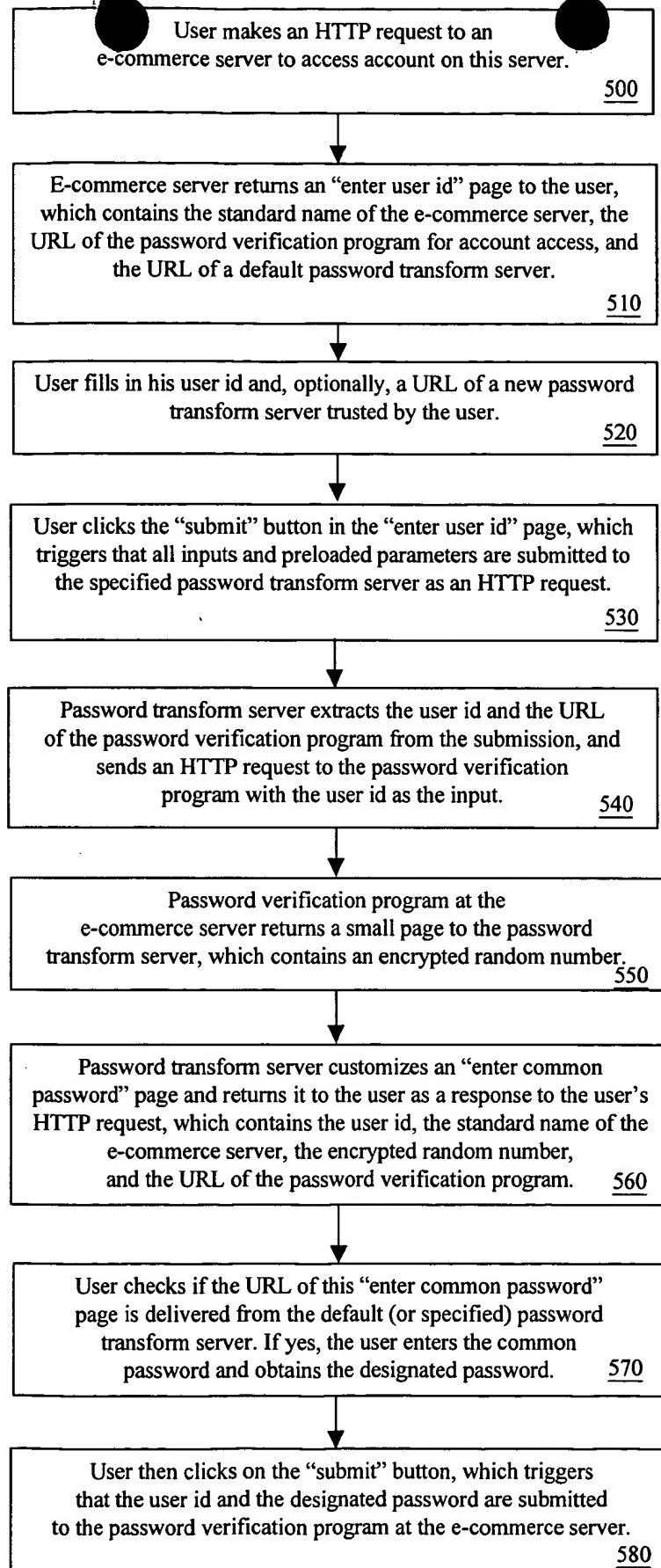


FIG. 6

Password Transform Web Interface - Netscape

File Edit View Go Communicator Help

Back Forward Reload Home Search Netscape Print Security

Bookmarks | Netsite: | http://project.onepass/OnePass.htm | What's Related

InstantMessage WebMail Contact People YellowPages Downloads

Common Password to Designated Password

1. Input account username:
2. Input account location:
3. Input common password:
4. Get designated password:

Document Done